(iii) Deputy Commander, Naval Legal Service Command.

(3) *In the Operating Forces.* All officers authorized by Article 22, Uniform Code of Military Justice (UCMJ), or designated in section 0120, Manual of the Judge Advocate General (JAGINST 5800.7C), to convene general courts-martial.

(f) *Review authority.* (1) The Assistant Secretary of the Navy (Manpower and Reserve Affairs), is the Secretary's designee, and shall act upon requests for administrative review of initial denials of requests for amendment of records related to fitness reports and performance evaluations of military personnel (see § 701.111(c)(3)).

(2) The Judge Advocate General and General Counsel, as the Secretary's designees, shall act upon requests for administrative review of initial denials of records for notification, access, or amendment of records, as set forth in § 701.111(c)(2) and (4).

(3) The authority of the Secretary of the Navy (SECNAV), as the head of an agency, to request records subject to the Privacy Act from an agency external to the Department of Defense for civil or criminal law enforcement purposes, under subsection (b)(7) of 5 U.S.C. 552a, is delegated to the Commandant of the Marine Corps, the Director of Naval Intelligence, the Judge Advocate General, and the General Counsel.

(g) *Systems manager.* Systems managers, as designated in Department of the Navy's compilation of systems notices (periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211[6], ''Current Privacy Act Issuances'') shall:

(1) Ensure the system has been published in the FEDERAL REGISTER and that any additions or significant changes are submitted to CNO (N09B30) for approval and publication. The systems of records should be maintained in accordance with the systems notices as published in the periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances.''

(2) Maintain accountability records of disclosures.

[6] See footnote 3 to § 701.101.

(h) *Department of the Navy employees.* Each employee of the Department of the Navy has certain responsibilities for safeguarding the rights of others. These include:

(1) Not disclosing any information contained in a system of records by any means of communication to any person or agency, except as authorized by this subpart and subpart G of this part.

(2) Not maintaining unpublished official files which would fall under the provisions of 5 U.S.C. 552a.

(3) Safeguarding the privacy of individuals and confidentiality of personal information contained in a system of records.

§ 701.105 Systems of records.

To be subject to this subpart and subpart G of this part, a ''system of records'' must consist of ''records'' that are retrieved by the name, or some other personal identifier, of an individual and be under the control of Department of the Navy.

(a) *Retrieval practices.* (1) Records in a group of records that are not retrieved by personal identifiers are not covered by this subpart and subpart G of this part, even if the records contain information about individuals and are under the control of Department of the Navy. The records must be retrieved by personal identifiers to become a system of records.

(2) If records previously not retrieved by personal identifiers are rearranged so they are retrieved by personal identifiers, a new system notice must be submitted in accordance with § 701.107.

(3) If records in a system of records are rearranged so retrieval is no longer by personal identifiers, the records are no longer subject to this subpart and subpart G of this part and the records system notice should be deleted in accordance with § 701.107.

(b) *Recordkeeping standards.* A record maintained in a system of records subject to this subpart and subpart G of this part must meet the following criteria:

(1) Be accurate. All information in the record must be factually correct.

(2) Be relevant. All information contained in the record must be related to the individual who is the record subject

and also must be related to a lawful purpose or mission of the Department of the Navy activity maintaining the record.

(3) Be timely. All information in the record must be reviewed periodically to ensure that it has not changed due to time or later events.

(4) Be complete. It must be able to stand alone in accomplishing the purpose for which it is maintained.

(5) Be necessary. All information in the record must be needed to accomplish a Department of the Navy mission or purpose established by Federal Law or E.O. of the President.

(c) *Authority to establish systems of records.* Identify the specific Federal statute or E.O. of the President that authorizes maintaining each system of records. When a naval activity uses its ''internal housekeeping'' statute, i.e., 5 U.S.C. 301, Departmental Regulations, the naval instruction that implements the statute should also be identified. A statute or E.O. authorizing a system of records does not negate the responsibility to ensure the information in the system of records is relevant and necessary.

(d) *Exercise of First Amendment rights.* (1) Do not maintain any records describing how an individual exercises rights guaranteed by the First Amendment of the U.S. Constitution unless expressly authorized by Federal law; the individual; or pertinent to and within the scope of an authorized law enforcement activity.

(2) First amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

(e) *System manager's evaluations and reviews.* (1) Evaluate each new system of records. Before establishing a system of records, evaluate the information to be included and consider the following:

(i) The relationship of each item of information to be collected and retained to the purpose for which the system is maintained (all information must be relevant to the purpose);

(ii) The specific impact on the purpose or mission if each category of information is not collected (all information must be necessary to accomplish a lawful purpose or mission.);

(iii) The ability to meet the informational needs without using personal identifiers (will anonymous statistical records meet the needs?);

(iv) The length of time each item of information must be kept;

(v) The methods of disposal;

(vi) The cost of maintaining the information; and

(vii) Whether a system already exists that serves the purpose of the new system.

(2) Evaluate and review all existing systems of records.

(i) When an alteration or amendment of an existing system is prepared pursuant to §701.107(b) and (c), do the evaluation described in §701.105(e).

(ii) Conduct the following reviews annually and be prepared to report, in accordance with §701.104(c)(8), the results and corrective actions taken to resolve problems uncovered.

(A) Training practices to ensure all personnel are familiar with the requirements of 5 U.S.C. 552a, and DoD Directive 5400.11, ''DoD Privacy Program'', this subpart and subpart G of this part, and any special needs their specific jobs entail.

(B) Recordkeeping and disposal practices to ensure compliance with this subpart and subpart G of this part.

(C) Ongoing computer matching programs in which records from the system have been matched with non-DoD records to ensure that the requirements of §701.115 have been met.

(D) Actions of Department of the Navy personnel that resulted in either Department of the Navy being found civilly liable or a person being found criminally liable under 5 U.S.C. 552a, to determine the extent of the problem and find the most effective way of preventing the problem from occurring in the future.

(E) Each system of records notice to ensure it accurately describes the system. Where major changes are needed, alter the system notice in accordance with §701.107(b). If minor changes are needed, amend the system notice pursuant to §701.107(c).

(iii) Every even-numbered year, review a random sample of Department of the Navy contracts that provide for

the operation of a system of records to accomplish a Department of the Navy function, to ensure the wording of each contract complies with the provisions of 5 U.S.C. 552a and § 701.105(h).

(iv) Every three years, beginning in 1992, review the routine use disclosures associated with each system of records to ensure the recipient's use of the records continues to be compatible with the purpose for which the information was originally collected.

(v) Every three years, beginning in 1993, review each system of records for which exemption rules have been established to determine whether each exemption is still needed.

(vi) When directed, send the reports through proper channels to the CNO (N09B30).

(f) *Discontinued information requirements.* (1) Immediately stop collecting any category or item of information about individuals that is no longer justified, and when feasible, remove the information from existing records.

(2) Do not destroy records that must be kept in accordance with retention and disposal requirements established under SECNAVINST 5212.5[7], ''Disposal of Navy and Marine Corps Records.''

(g) *Review records before disclosing outside the Federal government.* Before disclosing a record from a system of records to anyone outside the Federal government, take reasonable steps to ensure the record which is being disclosed is accurate, relevant, timely, and complete for the purposes it is being maintained.

(h) *Federal government contractors*—(1) *Applicability to Federal government contractors.* (i) When a naval activity contracts for the operation of a system of records to accomplish its function, the activity must ensure compliance with this subpart and subpart G of this part and 5 U.S.C. 552a. For the purposes of the criminal penalties described in 5 U.S.C. 552a, the contractor and its employees shall be considered employees of the agency during the performance of the contract.

(ii) Consistent with Parts 24 and 52 of the Federal Acquisition Regulation (FAR), contracts for the operation of a system of records shall identify specifically the record system and the work to be performed, and shall include in the solicitations and resulting contract the terms as prescribed by the FAR.

(iii) If the contractor must use records that are subject to this subpart and subpart G of this part to perform any part of a contract, the contractor activities are subject to this subpart and subpart G of this part.

(iv) This subpart and subpart G of this part do not apply to records of a contractor that are:

(A) Established and maintained solely to assist the contractor in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract;

(B) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to the naval activity;

(C) Maintained as training records by an educational organization contracted by a naval activity to provide training when the records of the contract students are similar to and commingled with training records of other students, such as admission forms, transcripts, and academic counseling and similar records; or

(D) Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with 31 U.S.C. 952d.

(v) For contracting that is subject to this subpart and subpart G of this part, naval activities shall publish instructions that:

(A) Furnish Privacy Act guidance to personnel who solicit, award, or administer Government contracts;

(B) Inform prospective contractors of their responsibilities under this subpart and subpart G of this part and the Department of the Navy Privacy Program;

(C) Establish an internal system for reviewing contractor's performance for compliance with the Privacy Act; and

(D) Provide for the biennial review of a random sample of contracts that are subject to this subpart and subpart G of this part.

(2) *Contracting procedures.* The Defense Acquisition Regulatory (DAR)

[7] Copies available from OPNAV/SECNAV Directives Control Office, Washington Navy Yard, Building 200, Washington, DC 20350–2000.

Council, which oversees the implementation of the FAR within the Department of Defense, is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts that are subject to this subpart and subpart G of this part and 5 U.S.C. 552a.

(3) *Contractor compliance.* Naval activities shall establish contract surveillance programs to ensure contractors comply with the procedures established by the DAR Council under the preceding subparagraph.

(4) *Disclosing records to contractors.* Disclosing records to a contractor for use in performing a contract let by a naval activity is considered a disclosure within Department of the Navy. The contractor is considered the agent of Department of the Navy when receiving and maintaining the records for that activity.

§ 701.106 Safeguarding records in systems of records.

Establish appropriate administrative, technical, and physical safeguards to ensure the records in every system of records are protected from unauthorized alteration, destruction, or disclosure. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(a) *Minimum standards.* (1) Conduct risk analysis and management planning for each system of records. Consider sensitivity and use of the records, present and projected threats and vulnerabilities, and present and projected cost-effectiveness of safeguards. The risk analysis may vary from an informal review of a small, relatively insensitive system to a formal, fully quantified risk analysis of a large, complex, and highly sensitive system.

(2) Train all personnel operating a system of records or using records from a system of records in proper record security procedures.

(3) Label information exempt from disclosure under this subpart and subpart G of this part to reflect their sensitivity, such as ''FOR OFFICIAL USE ONLY,'' ''PRIVACY ACT SENSITIVE: DISCLOSE ON A NEED-TO-KNOW BASIS ONLY,'' or some other statement that alerts individuals of the sensitivity to the records.

(4) Administer special administrative, physical, and technical safeguards to protect records processed or stored in an automated data processing or word processing system to protect them from threats unique to those environments.

(b) *Records disposal.* (1) Dispose of records from systems of records so as to prevent inadvertent disclosure. Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (i.e., such as tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

(2) The transfer of large volumes of records (e.g., printouts and computer cards) in bulk to a disposal activity such as a Defense Reutilization and Marketing Office for authorized disposal is not a disclosure of records, if the volume of records, coding of the information, or some other factor render it impossible to recognize any personal information about a specific individual.

(3) When disposing or destroying large quantities of records from a system of records, care must be taken to ensure that the bulk of the records is maintained to prevent easy identification of specific records. If such bulk is maintained, no special procedures are required. If bulk is not maintained, or if the form of the records makes individually identifiable information easily discernable, dispose of the records in accordance with § 701.106(b)(1).

§ 701.107 Criteria for creating, altering, amending and deleting Privacy Act systems of records.

(a) *Criteria for a new system of records.* A new system of records is one for which no existing system notice has been published in the FEDERAL REGISTER. If a notice for a system of records has been canceled or deleted, and it is determined that it should be reinstated or reused, a new system notice must be published in the FEDERAL REGISTER. Advance public notice must